

## TLS Certificate Chain Misconfiguration on webhosting-external.jpl.nasa.gov

From josephgoyd <josephgoyd@proton.me>

To soc@nasa.gov

Date Tuesday, April 22nd, 2025 at 4:04 PM

To the NASA Cybersecurity Team,

I am writing to report a TLS certificate chain misconfiguration affecting the domain:

<https://webhosting-external.jpl.nasa.gov>

While analyzing the certificate chain presented by this endpoint, I noticed that the intermediate certificate is issued by "Entrust OV TLS Issuing RSA CA 1", but the root certificate being presented is "SSL.com TLS RSA Root CA 2022". This appears to be a misconfiguration, as SSL.com and Entrust are distinct certificate authorities and should not be part of the same trust chain.

This mismatch causes trust validation errors in modern operating systems and browsers, flagging the connection as untrusted. This could result in user access issues and might also impact internal systems relying on TLS validation.

Impact:

- Users may be unable to securely connect to the site.
- Systems relying on automated certificate trust chains may reject the connection.
- Potential exposure to downgrade or interception attacks in permissive client configurations.

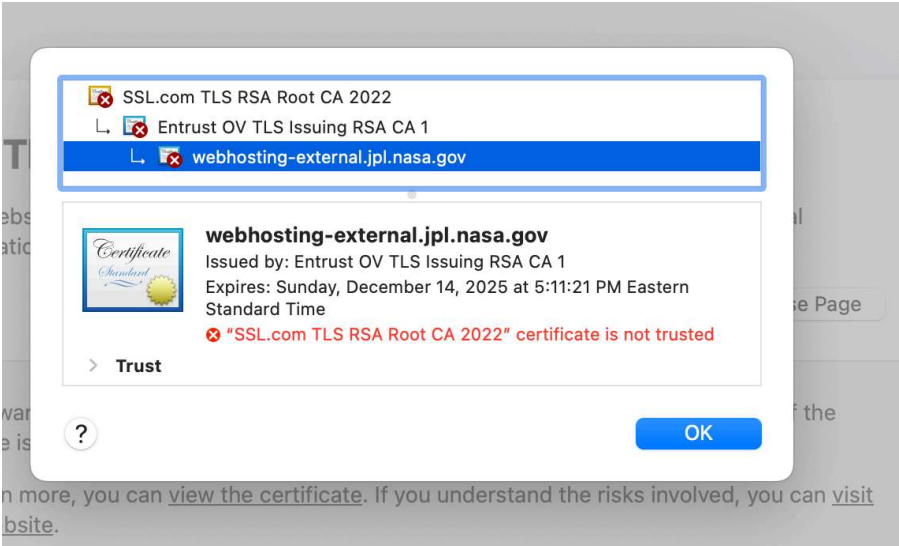
I've attached a screenshot that demonstrates the issue, along with OpenSSL output showing the full certificate chain as presented by the server.

Suggested Fix: Ensure that the correct root certificate corresponding to the Entrust intermediate is served by the server, or configure the full certificate chain correctly on the web server.

Please let me know if any additional information is needed or if I can assist further. I'm submitting this in the spirit of responsible disclosure to help improve the security posture of NASA services.

Best regards,  
Joseph Goydish

<https://www.linkedin.com/in/josephg007/>



244.51 KB    1 embedded image

Screen Shot 2025-04-22 at 6.41.43 PM.png 244.51 KB